

CLERK'S OFFICE

A TRUE COPY

Dec 03, 2020

s/ Jeremy Heacox

Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)A silver Alcatel cellular phone, model 5032W, IMEI# 015552000169949
in a black phone case that is currently in evidence under Inventory
3051-MW-3084413, Item #1B11, at FBI, St. Francis, WI.

Case No. 20-M-459 (SCD)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

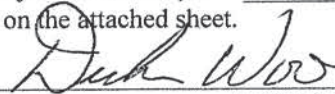
The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. Section 2252A	Possession and distribution child pornography

The application is based on these facts:

See attached affidavit

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

FBI Task Force Officer Dickson Woo

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
telephone _____ (specify reliable electronic means).

Date: 12-3-20

City and state: Milwaukee, WI



Judge's signature

Hon. Stephen C. Dries

Printed name and title

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Dickson Woo, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information stored electronically in a cellular telephone. The information to be searched is described in the following paragraphs and in Attachment A.

2. I am a Task Force officer with the Federal Bureau of Investigation (FBI), and have been since January 2015 I am assigned to the FBI's Child Exploitation Task Force, Milwaukee Division. My duties include investigating violations of federal criminal law, including violations of Title 18, United States Code, Section 2252, which criminalizes accessing with intent to view, possession, receipt, and distribution of child pornography. I have gained experience in conducting these investigations through training and through everyday work, to include executing search warrants and conducting interviews of individuals participating in the trading and manufacturing of child pornography. I have also received training relating to the investigation of Internet Crimes against Children (ICAC) which includes training in the investigation and enforcement of state and federal child pornography laws in which computers and other digital media are used as a means for receiving, transmitting, and storing child pornography.

3. As a Federal Task Force officer, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States. In particular I investigate violations of Title 18, United States Code, Sections 2251 and 2252A

which criminalize, among other things, the production, advertisement, possession, receipt, and transportation of child pornography.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2252A have been committed by Dennis Czysz, Jr. There is also probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

6. This affidavit is submitted in support of an application for a search warrant for the following portable electronic device (“Device”), which is currently in evidence at the Federal Bureau of Investigations (“FBI”) - Milwaukee Office, for evidence of the user’s possible involvement in possession and/or distribution of child pornography described in detail below:

- a. A silver Alcatel cellular phone, model 5032W, IMEI# 015552000169949 in a black phone case that is currently in evidence under Inventory 305I-MW-3084413, Item #1B11.

DEFINITIONS

7. The following definitions apply to the Affidavit and Attachment B to this Affidavit:

- a. “Cellular telephone” or “cell phone” means a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless

telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books”; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may include geolocation information indicating where the cell phone was at particular times.

b. “Child Pornography” is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

c. “Computer” is defined pursuant to 18 U.S.C. § 1030(e)(1) as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.”

d. “Computer Server” or “Server,” is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer that hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user’s computer via the Internet. A domain name system

(DNS) server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol (IP) address so the computer hosting the web site may be located, and the DNS server provides this function.

e. “Computer hardware” means all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

f. “Computer software” is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. “Computer-related documentation” consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

h. “Computer passwords, pass phrases and data security devices” consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A

password or pass phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

i. “Electronic storage devices” includes computers, cellular telephones, tablets, and devices designed specifically to store electronic information (e.g., external hard drives and USB “thumb drives”). Many of these devices also permit users to communicate electronic information through the internet or through the cellular telephone network (e.g., computers, cellular telephones, and tablet devices such as an iPad).

j. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

k. “Internet Service Providers” (ISPs) are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone-based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite-based subscription. ISPs typically charge a fee based upon the type of connection and volume of

data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a username or screen name, an “e-mail address,” an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider (ISP) over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

l. “An Internet Protocol address” (IP address) is a unique numeric address used by internet-enabled electronic storage devices to access the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every electronic storage device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that electronic storage device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static, that is, long-term IP addresses, while other computers have dynamic that is, frequently changed IP addresses.

m. “Hash Value” refers to the process of using a mathematical function, often called an algorithm, to generate a numerical identifier for data. A hash value can be thought of as a “digital fingerprint” for data. If the data is changed, even very slightly (like the addition or deletion of a comma or a period), the hash value changes. Therefore, if a file such as a digital photo is a hash value match to a known file, it means that the digital photo is an exact copy of the known file.

n. “Media Access Control” (MAC) address means a hardware identification number that uniquely identifies each device on a network. The equipment that connects a computer to a network is commonly referred to as a network adapter. Most network adapters

have a MAC address assigned by the manufacturer of the adapter that is designed to be a unique identifying number. A unique MAC address allows for proper routing of communications on a network. Because the MAC address does not change and is intended to be unique, a MAC address can allow law enforcement to identify whether communications sent or received at different times are associated with the same adapter.

o. “Minor” means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

p. The terms “records,” “documents,” and “materials” include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including writings and drawings), photographic form (including prints, negatives, videotapes, motion pictures, and photocopies), mechanical form (including printing and typing) or electrical, electronic or magnetic form (including tape recordings, compact discs, electronic or magnetic storage devices such as hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, smart cards, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

q. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

r. “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

PROBABLE CAUSE

8. The National Center for Missing and Exploited Children (NCMEC) provided NCMEC Cyber tip # 41119460 involving an individual who resides in the Milwaukee area and has a history of possessing child pornography. The complaint was filed by Dropbox to NCMEC on October 3, 2018. The complaint stated there were approximately 141 videos of suspected child pornography uploaded to the Dropbox account created by the email address of lauralraines@gmail.com, the screen name of Laural Raines, and the ESP user ID of 1027006608.

9. NCMEC served an administrative subpoena to Charter Communications for the IP address associated (2605:a000:b141:3400:a176:3fac:272a:f87a) with the Laural Raines Dropbox account for September 30, 2018. The IP address resolved to Dennis Czysz, 3657 E. Layton Avenue, Apt. 7, Cudahy, Wisconsin.

10. NCMEC served an administrative subpoena to Google, Inc. regarding the email address of lauralraines@gmail.com that was used to register for the Dropbox account. Google responded with that the email was listed to a Laural Raines, created on 04/13/2018 02:32:54-UTC, (414) 412-2487- T-Mobile, Google account number 417602629805.

11. NCMEC served an administrative subpoena to T-Mobile regarding the phone number of (414) 412-2487. T-Mobile responded with the subscriber information for the telephone number as listing to Dennis Czysz of 822 N. 24th Street, Milwaukee, WI 53233, Start time: Dec 15, 2017 08:00:00 (UTC), End time: Jan 01, 0001 08:00:00 (UTC).

12. A check on search databases such as CLEAR and Accurint showed Dennis Czysz resided at 3657 E. Layton Ave., Apt #7, Cudahy, WI in 2018. Through a check with the Wisconsin Department of Corrections (WI DOC) it showed Czysz as a registered sex offender in the State of Wisconsin and they had Dennis Czysz currently resided at 3803 W. National Ave.,

Apt. # 3, West Milwaukee, WI 53215. Dennis Czysz's Wisconsin Driver License also listed his address at 3803 W. National Ave., Apt # 3, West Milwaukee, WI. In 2000, he was convicted of exposing a child to harmful materials and in 2005 he was convicted of possession of child pornography. WI DOC also had Czysz's contact telephone number as (414) 412-2487.

13. On June 27, 2019, a Federal Search Warrant was executed at Dennis Czysz's address of 3803 W. National Ave, Apt #3, Milwaukee, WI. Czysz and two roommates were present at residence. Electronic devices and mediums such as laptops, cell phones and CD/DVD's were seized from the residence.

14. FBI CART (Computer Analysis Response Team) performed a forensic exam of the items, specifically the ZTE Z982 cell phone and a LG Model LM Q710MS, both having the cell phone number of (414) 412-2487 that were found on Czysz while at the residence. A review of the forensic image of the cell phones revealed approximately 1100 images and videos that were child pornography.

15. On October 20, 2020, Dennis Czysz was federally indicted on Possession of Child Pornography and Distribution of Child Pornography. An arrest warrant was issued for Czysz on these charges.

16. On November 3, 2020, Dennis Czysz was arrested on the federal arrest warrant near his residence of 1753 S. Kinnickinnic Ave., Milwaukee, WI. A search incident to arrest revealed a Black Alcatel cell phone, model 5032W, with phone number of 414-732-3696 in Czysz's right front coat pocket. Czysz refused to give consent for TFO Woo to search the cell phone.

17. As of November 10, 2020, there were a series of confirmed cases of COVID at the FBI-Milwaukee office and Task Force Offices were advised to avoid coming to the FBI-

Milwaukee for the next couple of weeks. This caused a delay in drafting the search warrant for Czysz's new cell phone. As of December 1, 2020, I was able to draft and forward the search warrant affidavit for review to Assistant United States Attorney Megan Paulson.

18. It is known that people that collect child pornography often use electronic devices such as cell phones, tablets, external hard drives and other media to store the child pornography images and videos for their personal use and/or distribution at their discretion. It is also known that people who collect child pornography often maintain the images and videos for long periods of time, (for months to years), so the person can view or distribute the images and videos again.

19. In this case, two prior cell phones that were in the possession of Czysz contained child pornography images and videos as stated in paragraph 14.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

20. I anticipate executing this warrant will reveal records and other information, including the contents of the cellular telephone, particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS:

21. Based on my knowledge, training, and experience, as well as my conversations with other Special Agents of the Federal Bureau of Investigation, who are experienced with electronic communication systems, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the devices. This information can sometimes be recovered with forensics tools.

22. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of use, who used it, and when.

23. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to, computer-assisted scans of the entire medium that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

24. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

25. Based on the facts contained within this affidavit, I believe that probable cause exists to search the Device, which is more particularly described in Attachment A, and which is currently located in evidence at the Federal Bureau of Investigations-Milwaukee Office, for evidence of the aforementioned Possession and/or distribution of Child Pornography.

ATTACHMENT A

Property to Be Searched

The following property is to be searched:

A silver Alcatel cellular phone, model 5032W, IMEI# 015552000169949 in a black phone case that is currently in evidence under Inventory 305I-MW-3084413, Item #1B11.

The Device is currently in evidence at the Federal Bureau of Investigations - Milwaukee Office, located at 3600 S. Lake Dr., St. Francis, WI.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Particular Items to be Seized

a. All records on the Device described in Attachment A that relate to violations of Title 18, United States Code, Section 2252A involving Dennis Czysz and any other subject, which was in active memory of the Device as of June 27, 2019, to include:

- a. any information related to possession / distribution of Child Pornography
- b. any web search information related to the offenses described above.
- c. Photographs and videos associated to Child Pornography.
- d. any communications via text messages, email, Facebook, Twitter, or other web-based applications between the subjects and others regarding the offenses described above; and
- e. all bank records, checks, credit card bills, account information, and other financial records.

b. Evidence of user attribution showing who used or owned the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of electronic storage and any photographic form.

Information to be seized by the government

All information described in the above documents that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 2252A involving the account(s) associated with the cellular telephone referenced in Attachment A pertaining to the possession and distribution of child pornography images and/or videos.